

New few weight codes from trace codes over a local Ring *

Minjia Shi

School of Mathematical Sciences, Anhui University, Hefei, 230601, China

National Mobile Communications Research Laboratory,

Southeast University, 210096, Nanjing, China

Liqin Qian

School of Mathematical Sciences, Anhui University, Hefei, 230601, China

Patrick Solé

CNRS/LAGA, University of Paris 8, 2 rue de la liberté, 93 Saint-Denis, France

Abstract

In this paper, new few weights linear codes over the local ring $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, with $u^2 = v^2 = 0, uv = vu$, are constructed by using the trace function defined over an extension ring of degree m . These trace codes have the algebraic structure of abelian codes. Their weight distributions are evaluated explicitly by means of Gaussian sums over finite fields. Two different defining sets are explored. Using a linear Gray map from R to \mathbb{F}_p^4 , we obtain several families of new p -ary codes from trace codes of dimension $4m$. For the first defining set: when m is even, or m is odd and $p \equiv 3 \pmod{4}$, we obtain a new family of two-weight codes, which are shown to be optimal by the application of the Griesmer bound; when m is even and under some special conditions, we obtain two new classes of three-weight codes. For the second defining set: we obtain a new class of two-weight codes and prove that it meets the Griesmer bound. In addition, we give the minimum distance of the dual code. Finally, applications of the p -ary image codes in secret sharing schemes are presented.

Keywords: Few weights codes; Gray map; Trace codes; Secret sharing schemes

*This research is supported by National Natural Science Foundation of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

1 Introduction

Let p denote an odd prime, and m, n be positive integers. Let $D = \{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}_{p^m}^*$. Define a p -ary linear code of length n as $C_D = \{(tr(xd_1), tr(xd_2), \dots, tr(xd_n)) : x \in \mathbb{F}_{p^m}\}$, where $tr()$ is the absolute trace function of \mathbb{F}_{p^m} down to \mathbb{F}_p . Here, D is called the **defining set** of C_D . The code C_D may have good parameters if the set D is well chosen. In the sense, this construction is generic. Some linear codes over \mathbb{F}_p can be constructed in this method, and few weights codes [11, 12] can be produced by suitably selecting the defining set D . Hence, the selection of D directly effects the construction of linear codes. Although the defining set of our abelian code is not a cyclic group, it is an abelian group.

Since the 1970s, two-weight codes over fields have been studied, thanks to their connections to strongly regular graphs, difference sets, and finite geometries. Two-weight codes over fields are discussed in [4], two-weight codes over rings are surveyed in [2]. In this paper, we have obtained several classes of linear codes with few weights over a special ring by using a trace function over a local ring \mathcal{R} which is an m -extension of the alphabet ring R . Two different defining sets are explored for these trace codes: L , a natural lift of the D above from the residue field of \mathcal{R} to \mathcal{R} , and L' the full unit group of \mathcal{R} . Codes over finite fields are obtained from that data by Gray mapping. In [18, 19, 20, 21, 22], by different choices of the defining set, we get two-weight or three-weight codes over various rings. Linear codes with few weights have applications in Massey's secret sharing scheme [8], association schemes and difference sets [3, 5], in addition to their standard applications in communication and data storage systems. Hence, linear codes with few weights are a very interesting research topic in coding theory, and has been investigated in [6, 7, 9, 12].

In the present paper, motivated by the research work listed in [3, 6], we construct trace codes over an extension ring of degree m of the alphabet $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, then this leads us to construct linear codes over \mathbb{F}_p with few weights by using the Gray map. When $N_2 = 1$, in the case of m even, or if m is odd, in the case of $p \equiv 3 \pmod{4}$, we obtain a two-weight code, which is shown to be optimal by the application of Griesmer bound [13]. The aforementioned works lead us to the study of few weights codes and their weight enumerators over rings. The contribution of this paper is twofold. First, we present two families of optimal two-weight codes, and show their application of secret sharing schemes. Next, we obtain two-weight codes and three-weight codes with new parameters, that are different from those of [10, 15, 18, 19, 22]. More precisely, we summarize our results as follows. To this end, we begin to give some notations.

1.1 Some notations fixed throughout this paper

First, we introduce some notations valid for the whole paper.

- Let \mathbb{F}_p be the finite field of p elements with characteristic p . p is an odd prime.
- Let $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. Denote a m -extension ring of R by \mathcal{R} , and the trace map from \mathcal{R} to R by Tr . Precisely, for any $x \in \mathbb{F}_{p^m}$, the trace tr of x is $tr(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}$, i.e., tr is the **trace function** from \mathbb{F}_{p^m} to \mathbb{F}_p .
- For any $x \in R^n$, $w_L(x)$ denotes the Lee weight of x , $w_H(x)$ denotes the Hamming weight of x .
- Let N be a positive integer such that $N|(p^m - 1)$. Let $N_1 = \text{lcm}(N, \frac{p^m-1}{p-1})$ and $N_2 = \text{gcd}(N, \frac{p^m-1}{p-1})$.
- C_i^N denotes the **cyclotomic classes** of order N in \mathbb{F}_{p^m} .
- $\Re(\Delta)$ denotes the **real part** of the complex number Δ .

1.2 Statement of main results

In this paper, we define two different defining sets:

$$\begin{aligned} L &= \{a + bu + cv + duv : a \in D, b, c, d \in \mathbb{F}_{p^m}\} \subseteq \mathcal{R}^*; \\ L' &= \{a + bu + cv + duv : a \in \mathbb{F}_{p^m}^*, b, c, d \in \mathbb{F}_{p^m}\} = \mathcal{R}^*. \end{aligned}$$

Thus $|L| = np^{3m}$ and $|L'| = (p^m - 1)p^{3m}$. For a fixed element $r \in \mathcal{R}$, the vectors $Ev(r), Ev'(r)$ are given by the **evaluation map**

$$Ev(r) = (Tr(rx))_{x \in L}, Ev'(r) = (Tr(rx))_{x \in L'},$$

respectively. Define the codes $C(m, p), C'(m, p)$ by the formulas $C(m, p) = \{Ev(r) | r \in \mathcal{R}\}, C'(m, p) = \{Ev'(r) | r \in \mathcal{R}\}$, respectively. Let M denote its maximal ideal, i.e., $M = \{bu + cv + duv : b, c, d \in \mathbb{F}_{p^m}\}$. The residue field \mathcal{R}/M is isomorphic to \mathbb{F}_{p^m} . It is obvious that \mathcal{R}^* is not cyclic, and that $\mathcal{R} = \mathcal{R}^* \cup M$.

Now, we calculate the Lee weight distributions of the code $C(m, p)$ and $C'(m, p)$, respectively.

Theorem 1.1 Let $N_2 = 1$, m is even or m is odd and $p \equiv 3 \pmod{4}$.

(a) **Defining set L with $|L| = np^{3m}$.** Then we have

- (i) If $r = 0$, then $w_L(Ev(r)) = 0$;
- (ii) If $r \in M \setminus \{0\}$,
 - 1) $r = \alpha uv$, where $\alpha \in \mathbb{F}_{p^m}^*$, then $w_L(Ev(r)) = 4p^{4m-1}$;
 - 2) $r \in M \setminus \{\alpha uv : \alpha \in \mathbb{F}_{p^m}^*\}$, then $w_L(Ev(r)) = 4p^{4m-1} - 4p^{3m-1}$;

(iii) If $r \in \mathcal{R}^*$, then $w_L(Ev(r)) = 4p^{4m-1} - 4p^{3m-1}$.

(b) **Defining set L' with $|L'| = (p^m - 1)p^{3m}$.** Then we have

- (i) If $r = 0$, then $w_L(Ev'(r)) = 0$;
- (ii) If $r \in M \setminus \{0\}$,
 - 1) $r = \alpha uv$, where $\alpha \in \mathbb{F}_{p^m}^*$, then $w_L(Ev'(r)) = 4(p-1)p^{4m-1}$;
 - 2) $r \in M \setminus \{\alpha uv : \alpha \in \mathbb{F}_{p^m}^*\}$, then $w_L(Ev'(r)) = 4(p-1)(p^{4m-1} - p^{3m-1})$;
- (iii) If $r \in \mathcal{R}^*$, then $w_L(Ev'(r)) = 4(p-1)(p^{4m-1} - p^{3m-1})$.

Next, we consider the case: $N_2 > 1$ and $|L| = np^{3m}$, as follows.

Theorem 1.2 Let m is even or m is odd and $p \equiv 3 \pmod{4}$. If $1 < N_2 < \sqrt{p^m} + 1$, then $C(m, p)$ is a $(|L|, p^{4m'}, d_L)$ linear code over R , which has at most $N_2 + 1$ nonzero Lee weights, where $m' \leq m$ and

$$\frac{4p^{3m-1}[p^m - (N_2 - 1)p^{\frac{m}{2}}]}{N_2} \leq d_L(C(m, p)) \leq \frac{4p^{3m-1}(p^m - 1)}{N_2}.$$

If there exists a positive integer l such that $p^l \equiv -1 \pmod{N_2}$, then the weight distribution of $C(m, p)$ is given below.

Theorem 1.3 Let m even and $N_2 = \gcd(N, \frac{p^m - 1}{p - 1}) > 2$ with $N|(p^m - 1)$. Assume that there exists a positive integer l such that $p^l \equiv -1 \pmod{N_2}$. Denote $t = \frac{m}{2l}$.

- (1) Assuming that p, t , and $\frac{p^l + 1}{N_2}$ are odd, then the linear code $C(m, p)$ is a three-weight linear code, where N_2 is even and $N_2 < p^{\frac{m}{2}} + 1$. The weights of $C(m, p)$ are presented in Table I.

Table I. Weight distribution of $C(m, p)$

Weight	Frequency
0	1
$\frac{4p^{3m-1}[p^m - (N_2 - 1)p^{\frac{m}{2}}]}{N_2}$	$\frac{p^m - 1}{N_2}$
$\frac{4p^{3m-1}(p^m - 1)}{N_2}$	$p^{3m}(p^m - 1)$
$\frac{4p^{3m-1}[p^m + p^{\frac{m}{2}}]}{N_2}$	$\frac{(N_2 - 1)(p^m - 1)}{N_2}$

- (2) In all other cases, the linear code $C(m, p)$ is a three-weight linear code, where $p^{\frac{m}{2}} + (-1)^t(N_2 - 1) > 0$. The weights of $C(m, p)$ are presented in Table II.

Table II. Weight distribution of $C(m, p)$

Weight	Frequency
0	1
$\frac{4p^{3m-1}[p^m+(-1)^t(N_2-1)p^{\frac{m}{2}}]}{N_2}$	$\frac{p^m-1}{N_2}$
$\frac{4p^{3m-1}(p^m-1)}{N_2}$	$p^{3m}(p^m-1)$
$\frac{4p^{3m-1}[p^m-(-1)^t p^{\frac{m}{2}}]}{N_2}$	$\frac{(N_2-1)(p^m-1)}{N_2}$

The manuscript is organized as follows. Section 2 presents some definitions and known facts, which will be needed in the rest of the paper. The proofs of Theorems 1.1, 1.2 and 1.3, together with some lemmas, corollaries and examples, are presented in Section 3. Section 4 determines the minimum distance of the dual codes. Furthermore, the optimality and applications to secret sharing schemes are discussed in Section 5. By using Gray map, two-weight codes we obtain meet the Griesmer bound with equality. In Section 6, we summarize this paper, and give some conjectures which are worth studying in the future.

2 Preliminaries

2.1 The trace function of the extension ring

Throughout this paper, we consider the ring $R = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, with p^4 elements, where $u^2 = v^2 = 0, uv = vu$. Given a positive integer m , we construct an extension of R with degree m as $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + uv\mathbb{F}_{p^m}$. There is a *Frobenius operator* F which maps $a + bu + cv + duv$ onto $a^p + b^p u + c^p v + d^p uv$. The *Trace*, denoted by Tr , of $a + bu + cv + duv$ over \mathcal{R} is defined as $Tr = \sum_{j=0}^{m-1} F^j$. It is then immediate to check that

$$Tr(a + bu + cv + duv) = tr(a) + tr(b)u + tr(c)v + tr(d)uv,$$

for $a, b, c, d \in \mathbb{F}_{p^m}$, where $tr()$ denotes the trace function from \mathbb{F}_{p^m} onto \mathbb{F}_p , and it is easy to verify that Tr is linear.

2.2 Gray map

From R to \mathbb{F}_p^4 , the Gray map Φ is defined as:

$$\Phi(a + bu + cv + duv) = (d, c + d, b + d, a + b + c + d),$$

where $a, b, c, d \in \mathbb{F}_p$. This map Φ can be extended to R^n in an obvious way. The Lee weight is defined as the Hamming weight of Gray image

$$w_L(a + bu + cv + duv) = w_H(a) + w_H(c + d) + w_H(b + d) + w_H(a + b + c + d),$$

for $a, b, c, d \in \mathbb{F}_p$. The Lee distance of $x, y \in R^n$ is defined as $w_L(x - y)$. As was observed in [22], Φ is a distance preserving isometry map from (R^n, d_L) to (\mathbb{F}_p^{4n}, d_H) , where d_L and d_H denote the **Lee distance** and **Hamming distance** in R^n and \mathbb{F}_p^{4n} , respectively. Moreover, if C is a linear code over R with parameters (n, p^k, d) , then $\Phi(C)$ is a linear code of parameters $[4n, k, d]$ over \mathbb{F}_p .

2.3 Abelian codes

A code over R is an ideal in the group ring $R[G]$, where G is a finite abelian group, so we call the code is **abelian**. In short, the coordinates of the codes C are indexed by elements of G and G acts regularly on this set. In the special case when G is cyclic, the code is a cyclic code in the usual sense [16]. Note that $C(m, p)$ is a code of length $|L| = \frac{N_1 p^{3m}}{N}$, over R .

Lemma 2.1 For all $x \in L$ (resp. L'), if $Tr(rx) = 0$, then $r = 0$.

Proof. Let $x = x_0 + x_1u + x_2v + x_3uv, r = r_0 + r_1u + r_2v + r_3uv$, where $x_0 \in D \subseteq \mathbb{F}_{p^m}^*, x_i \in \mathbb{F}_{p^m}, i = 1, 2, 3$ and $r_j \in \mathbb{F}_{p^m}, j = 0, 1, 2, 3$. By a direct computation we have

$$\begin{aligned} rx &= r_0x_0 + (r_0x_1 + r_1x_0)u + (r_0x_2 + r_2x_0)v + (r_0x_3 + r_1x_2 + r_2x_1 + r_3x_0)uv \\ &=: A_1 + A_2u + A_3v + A_4uv. \end{aligned}$$

Then $Tr(rx) = 0$ is equivalent to $tr(A_k) = 0, k = 1, 2, 3, 4$. Applying the nondegenerate character of $tr()$ [16], we can get $r_j = 0, j = 0, 1, 2, 3$, i.e., $r = 0$. Hence, the proof is completed. Similarly, since $L \subseteq L'$, the conclusion holds if replacing L by L' . \square

The following result is a simple generalization of Proposition 1 in [22], we omit the proof here.

Proposition 2.2 The group L (resp. L') acts regularly on the coordinates of $C(m, p)$ (resp. $C'(m, p)$).

The code $C(m, p)$ (resp. $C'(m, p)$) is thus an *abelian code* with respect to the group L (resp. L'). In other words, it is an ideal of the group ring $R[L]$ (resp. $R[L']$). As observed in the previous section, L (resp. L') is a not cyclic group, hence $C(m, p)$ (resp. $C'(m, p)$) may be not cyclic. The next result shows that its Gray image is also abelian.

Proposition 2.3 A finite group of size $4|L|$ (resp. $4|L'|$) acts regularly on the coordinates of $\Phi(C(m, p))$ (resp. $\Phi(C'(m, p))$).

Proof. This result we can obtain by the similar proof of Proposition 3.2 in [21]. \square

2.4 The weight formulas and character sums

Next, keeping the notation as before, we will be involved with Gaussian sums, which are arguably the most important types of exponential sums for finite fields, as they control the interplay between the additive and the multiplicative structure.

Denote the canonical additive characters of \mathbb{F}_p and \mathbb{F}_{p^m} by ϕ, χ , respectively. Denote arbitrary multiplicative characters of \mathbb{F}_p and \mathbb{F}_{p^m} by λ, ψ , respectively. The **Gaussian sums** [14] over \mathbb{F}_p and \mathbb{F}_{p^m} are defined respectively by

$$G(\lambda, \phi) = \sum_{x \in \mathbb{F}_p^*} \lambda(x) \phi(x), \quad G(\psi, \chi) = \sum_{x \in \mathbb{F}_{p^m}^*} \psi(x) \chi(x).$$

These sums are of particular importance for the proofs of Section 3.

Now we introduce a lemma about abelian groups.

Lemma 2.4 [12, Lemma 3.1] Let H and K be two subgroups of a finite abelian group G . Then $h_1 K = h_2 K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$ for $h_1, h_2 \in H$. Moreover, there is an isomorphism: $HK/K \cong H/(H \cap K)$ and $[HK : K] = [H : (H \cap K)]$, where $HK = \{hk : h \in H, k \in K\}$.

Let ξ be a fixed primitive element of \mathbb{F}_{p^m} and $\mathbb{F}_{p^m}^* = \langle \xi \rangle$, $\langle \xi^N \rangle$ denote the subgroup of $\mathbb{F}_{p^m}^*$. Define $C_i^N = \xi^i \langle \xi^N \rangle$, $i = 0, 1, \dots, N-1$. Denoted $C_0^N = \langle \xi^N \rangle$ by H and $\mathbb{F}_p^* = \langle \xi^{\frac{p^m-1}{p-1}} \rangle$ by K . Then we have $H \cap K = C_0^{N_1}$ and $HK = C_0^{N_2}$. Let $n = [H : (H \cap K)] = |H|/|H \cap K| = N_1/N$. There is a coset decomposition of H as follows:

$$H = \bigcup_{j=1}^n h_j (H \cap K),$$

where $h_j = \xi^{N(j-1)}$, $j = 1, 2, \dots, n$.

- **The First Formula.** In terms of Lemma 2.4, we have the coset decomposition of HK :

$$HK = \bigcup_{j=1}^n h_j K. \tag{1}$$

Define $d_j = h_j = \xi^{N(j-1)}$ for $j = 1, 2, \dots, n$, where $n = \frac{N_1}{N}$. Then

$$D = \{d_j = \xi^{N(j-1)} : j = 1, 2, \dots, n\} \subseteq C_0^N \subseteq \mathbb{F}_{p^m}.$$

In the light of (1), d_1, d_2, \dots, d_n form a complete set of coset representatives of the factor group $C_0^{N_2}/\mathbb{F}_p^*$.

- **The Second Formula.** For a nonzero codeword $c_b = (tr(bd_1), tr(bd_2), \dots, tr(bd_n)) \in C_D$, $b \in \mathbb{F}_{p^m}^*$, where the definition of C_D has been introduced in the front of Section 1, i.e.,

$$C_D = \{(tr(xd_1), tr(xd_2), \dots, tr(xd_n)) : x \in \mathbb{F}_{p^m}\}. \quad (2)$$

Let $w_H(c_b)$ denote its Hamming weight. Note that C_D is punctured from the linear code defined in [22] up to coordinate permutations. Then, we define a function of $b \in \mathcal{R}$ as follows. Let

$$N(b) = |\{1 \leq j \leq n : tr(bd_j) = 0\}|,$$

and thus the Hamming weight of the codeword attached to b is $w_H(c_b) = n - N(b)$. From the basic facts of additive characters and Formula (1), we have a similar formula in [12] as follows:

$$pN(b) = n + \frac{1}{N_2(p^m - 1)} \sum_{\psi \in \hat{\mathbb{F}}_{p^m}^*} G(\bar{\psi}, \chi) \psi(b) \sum_{x \in \mathbb{F}_{p^m}^*} \psi(x^{N_2}).$$

In the light of the orthogonally property of multiplicative characters [14],

$$\sum_{x \in \mathbb{F}_{p^m}^*} \psi(x^{N_2}) = \begin{cases} p^m - 1, & \text{if } \psi^{N_2} = \psi_0 \text{ (trivial characters of } \mathbb{F}_{p^m}), \\ 0, & \text{otherwise.} \end{cases}$$

Hence, we have the following formula.

- **The Third Formula.**

$$pN(b) = n + \frac{1}{N_2} \sum_{j=0}^{N_2-1} G(\bar{\varphi}^j, \chi) \varphi^j(b), \quad (3)$$

where φ is a multiplicative character of order N_2 in $\hat{\mathbb{F}}_{p^m}^*$. Here, $\hat{\mathbb{F}}_{p^m}^*$ denotes multiplicative character group.

3 Proofs of the main results

Our task is to prove Theorems 1.1, 1.2 and 1.3. Let $\eta = \exp(\frac{2\pi i}{p})$ and $s = 4|L| = \frac{4N_1 p^{3m}}{N}$, $s' = 4|L'| = 4(p^m - 1)p^{3m}$. If $y = (y_1, y_2, \dots, y_N) \in \mathbb{F}_p^{\mathcal{N}}$. Define

$$\Theta(y) = \sum_{j=1}^{\mathcal{N}} \eta^{y_j}.$$

To keep things simple, we let $\theta(r) = \Theta(\Phi(Ev(r)))$, and $\theta'(r) = \Theta(\Phi(Ev'(r)))$. By linearity of the Gray map, and of the evaluation map, we see that $\theta(\tau r) = \Theta(\Phi(Ev(\tau r)))$, $\theta'(\tau r) = \Theta(\Phi(Ev'(\tau r)))$ for any $\tau \in \mathbb{F}_p^*$.

In order to determine the Lee weight of codewords of the code $C(m, p)$ and $C'(m, p)$, we first recall the following lemmas, which play an important role in the proofs of the main results.

Lemma 3.1 [22, Lemma 1] For all $y = (y_1, y_2, \dots, y_N) \in \mathbb{F}_p^N$, we have $\sum_{\tau=1}^{p-1} \Theta(\tau y) = (p-1)N - pw_H(y)$.

In the light of Lemma 3.1 and the definition of the Gray map, for $Ev(r) \in C(m, p)$, we have

$$w_L(Ev(r)) = \frac{(p-1)s - \sum_{\tau=1}^{p-1} \Theta(\tau \Phi(Ev(r)))}{p} = \frac{(p-1)s - \sum_{\tau=1}^{p-1} \theta(\tau r)}{p}. \quad (4)$$

For $Ev'(a) \in C'(m, p)$, we can get a similar equation that $s = s', Ev(a) = Ev'(r), \theta(\tau r) = \theta'(\tau r)$.

Lemma 3.2 [22, Lemma 2] If $p \equiv 3 \pmod{4}$, then $\sum_{\tau=1}^{p-1} \theta(\tau a) = (p-1)\Re(\theta(a))$.

Lemma 3.3 [16, Lemma 9, p. 143] If $z \in \mathbb{F}_{p^m}^*$, then $\sum_{x \in \mathbb{F}_{p^m}} \eta^{tr(zx)} = 0$.

The proof of Theorem 1.1 is given below.

Proof of Theorem 1.1 Assume that $\mathbb{F}_{p^m}^* = \langle \xi \rangle$, where ξ be a primitive element of \mathbb{F}_{p^m} . Then we obtain $\mathbb{F}_p^* = \langle \xi^{\frac{p^m-1}{p-1}} \rangle$. Let $x = x_0 + ux_1 + vx_2 + uvx_3$, where $x_0 \in D, x_1, x_2, x_3 \in \mathbb{F}_{p^m}$.

(a) Defining set L with $|L| = np^{3m}$.

(i) If $r = 0$, then $Ev(r) = \underbrace{(0, 0, \dots, 0)}_{|L|}$. Thus $w_L(Ev(r)) = 0$.

(ii) If $r \in M \setminus \{0\}$, we discuss this condition in two cases.

1) if $r = \alpha uv$, where $\alpha \in \mathbb{F}_{p^m}^*$. Then $rx = \alpha x_0 uv$ and $Tr(rx) = tr(\alpha x_0)uv$. By using the Gray map, we have

$$\Phi(Ev(r)) = (tr(\alpha x_0), tr(\alpha x_0), tr(\alpha x_0), tr(\alpha x_0))_{x_0, x_1, x_2, x_3}.$$

Since Φ is an isometry, then $w_L(Ev(r)) = w_H(\Phi(Ev(r))) = 4p^{3m}(n - N(\alpha))$, where $N(\alpha) = |\{1 \leq j \leq n : tr(d_j \alpha) = 0\}|$. Due to $N_2 = 1$ and the third formula, we obtain $pN(\alpha) = \frac{p^m - p}{p-1}$, which implies $w_L(Ev(r)) = 4p^{4m-1}$.

2) if $r \in M \setminus \{\alpha uv : \alpha \in \mathbb{F}_{p^m}^*\}$, let $r = \beta u$, where $\beta \in \mathbb{F}_{p^m}^*$, then $Tr(rx) = tr(\beta x_0)u + tr(\beta x_2)uv$. Taking the Gray map yields

$$\Phi(Ev(r)) = (tr(\beta x_2), tr(\beta x_2), tr(\beta x_0) + tr(\beta x_2), tr(\beta x_0) + tr(\beta x_2))_{x_0, x_1, x_2, x_3}.$$

According to Lemma 3.3 and applying character sums, we have

$$\theta(r) = 2 \sum_{x_0 \in D} \sum_{x_1 \in \mathbb{F}_{p^m}} \sum_{x_2 \in \mathbb{F}_{p^m}} \sum_{x_3 \in \mathbb{F}_{p^m}} \eta^{tr(\beta x_2)} + 2 \sum_{x_0 \in D} \sum_{x_1 \in \mathbb{F}_{p^m}} \sum_{x_2 \in \mathbb{F}_{p^m}} \sum_{x_3 \in \mathbb{F}_{p^m}} \eta^{tr(\beta x_0) + tr(\beta x_2)} = 0.$$

When m is even, then $2 \mid \frac{p^m-1}{p-1}$ and $\tau \in \mathbb{F}_p^*$ is a square in \mathbb{F}_{p^m} , which implies $\theta(\tau r) = \theta(r)$. By using Formula (4), we obtain $w_L(Ev(r)) = \frac{(p-1)s}{p} = 4p^{4m-1} - 4p^{3m-1}$.

When m is odd and $p \equiv 3 \pmod{4}$, by using Lemma 3.2, we have $\sum_{\tau=1}^{p-1} \theta(\tau r) = 0$ and $w_L(Ev(r)) = \frac{(p-1)s}{p} = 4p^{4m-1} - 4p^{3m-1}$.

Likewise, for $r \in \{\alpha u, \alpha u + \beta v, \alpha u + \beta uv, \alpha v + \beta uv, \alpha u + \beta v + \gamma uv, \text{ where } \alpha, \beta, \gamma \in \mathbb{F}_{p^m}^*\}$, we also obtain $w_L(Ev(r)) = \frac{(p-1)s}{p} = 4p^{4m-1} - 4p^{3m-1}$.

(iii) If $r \in R^*$, let $r = r_0 + r_1 u + r_2 v + r_3 uv$, where $r_0 \in \mathbb{F}_{p^m}^*, r_1, r_2, r_3 \in \mathbb{F}_{p^m}$. By a simple calculation, we get $Tr(rx) = tr(r_0 x_0) + tr(r_0 x_1 + r_1 x_0)u + tr(r_0 x_2 + r_2 x_0)v + tr(r_0 x_3 + r_1 x_2 + r_2 x_1 + r_3 x_0)uv =: B_0 + B_1 u + B_2 v + B_3 uv$. Taking the Gray map yields $\Phi(Ev(r)) = (B_3, B_2 + B_3, B_1 + B_3, B_0 + B_1 + B_2 + B_3)_x$. By using Lemma 3.2, we get $\theta(r) = 0$. Similar to the proof of 2), we obtain $w_L(Ev(r)) = \frac{(p-1)s}{p} = 4p^{4m-1} - 4p^{3m-1}$.

(b) Defining set L' with $|L'| = (p^m - 1)p^{3m}$.

The cases (i) and (iii) are like in the proof of (a). Next, we just prove (ii).

$$1) \text{ From 1) in the case (a), we have } \theta'(r) = 4 \sum_{x_0 \in \mathbb{F}_{p^m}^*} \sum_{x_1, x_2, x_3 \in \mathbb{F}_{p^m}} \eta^{tr(\alpha x_0)} = -4p^{3m}.$$

When m is even, then $2 \mid \frac{p^m-1}{p-1}$ and $\tau \in \mathbb{F}_p^*$ is a square in \mathbb{F}_{p^m} , which implies $\theta'(\tau r) = \theta'(r)$.

$$\text{By using Formula (4), we obtain } w_L(Ev'(r)) = \frac{(p-1)s' - \sum_{\tau=1}^{p-1} \theta'(\tau a)}{p} = 4(p-1)p^{4m-1}.$$

When m is odd and $p \equiv 3 \pmod{4}$, by using Lemma 3.2, we have $\sum_{\tau=1}^{p-1} \theta'(\tau r) = -4(p-1)p^{3m}$ and $w_L(Ev'(r)) = \frac{(p-1)s' + 4(p-1)p^{3m}}{p} = 4(p-1)p^{4m-1}$.

2) Similar to the proof of 2) in the case (a), we obtain $w_L(Ev'(r)) = \frac{(p-1)s'}{p} = 4(p-1)(p^{4m-1} - p^{3m-1})$. \square

Remark 1 In terms of Theorem 1.1, we have constructed a p -ary code of length $s = \frac{4(p^m-1)p^{3m}}{p-1}$, dimension $4m$. The two nonzero weights $\omega_1 < \omega_2$ of values $\omega_1 = 4p^{4m-1} - 4p^{3m-1}, \omega_2 = 4p^{4m-1}$, with respective frequencies f_1, f_2 given by $f_1 = p^{4m} - p^m, f_2 = p^m - 1$. Then the code $C(m, p)$ is a two-weight code and its weights are given in Table III.

Table III. Weight distribution of $C(m, p)$

Weight	Frequency
0	1
$4p^{4m-1}$	$p^m - 1$
$4p^{4m-1} - 4p^{3m-1}$	$p^{4m} - p^m$

Comparing parameters in [20], it is easy to see that the corresponding dimension is the same. However, the length, the weights and the frequencies of the code $C(m, p)$ are different.

Example 3.4 Let $(p, m) = (3, 2)$, the code $\Phi(C(2, 3))$ has parameters $[11664, 8, 7776]$ and its weight enumerator $1 + 6552x^{7776} + 8x^{8748}$ from Table III.

Example 3.5 Let $(p, m) = (3, 3)$, the code $\Phi(C(3, 3))$ has parameters $[1023516, 12, 682344]$ and its weight enumerator $1 + 531414x^{682344} + 26x^{708588}$ from Table III.

Remark 2 In terms of Theorem 1.1, we have constructed a p -ary code of length $s' = 4(p^m - 1)p^{3m}$, dimension $4m$. The two nonzero weights $\omega'_1 < \omega'_2$ of values $\omega'_1 = 4(p - 1)(p^{4m-1} - p^{3m-1})$, $\omega'_2 = 4(p - 1)p^{4m-1}$, with respective frequencies f'_1, f'_2 given by $f'_1 = p^{4m} - p^m$, $f'_2 = p^m - 1$. Then the code $C'(m, p)$ is a two-weight code and its weights are given in Table III'.

Table III'. Weight distribution of $C'(m, p)$

Weight	Frequency
0	1
$4(p - 1)p^{4m-1}$	$p^m - 1$
$4(p - 1)(p^{4m-1} - p^{3m-1})$	$p^{4m} - p^m$

Comparing parameters in [21], it is not hard to see that the corresponding dimension and frequency are the same. However, the length and the weights of the code $C'(m, p)$ are different.

Example 3.6 Let $(p, m) = (3, 2)$, the code $\Phi(C'(2, 3))$ has parameters $[23328, 8, 15552]$ and its weight enumerator $1 + 6552x^{15552} + 8x^{17496}$ from Table III'.

Taking $q = p$ in Theorem 4.1 of [12], then we can obtain the following corollary.

Corollary 3.7 Let m is even and $N_2 = \gcd(N, \frac{p^m - 1}{p - 1}) > 2$, where $N | (p^m - 1)$. Assume that there exists a positive integer l such that $p^l \equiv -1 \pmod{N_2}$. Denote $t = \frac{m}{2l}$.

- (1) If N_2 is even, p, t , and $\frac{p^l + 1}{N_2}$ are odd, then the linear code C_D defined in Formula (2) is a two-weight $[\frac{N_1}{N}, m]$ linear code provided that $N_2 < p^{\frac{m}{2}} + 1$, with two nonzero weights are given in Table IV.

Table IV. Weight distribution of C_D

Weight	Frequency
0	1
$\frac{p^m - (N_2 - 1)p^{\frac{m}{2}}}{pN_2}$	$\frac{p^m - 1}{N_2}$
$\frac{p^m + p^{\frac{m}{2}}}{pN_2}$	$\frac{(N_2 - 1)(p^m - 1)}{N_2}$

- (2) In all other cases, the linear code C_D defined in Formula (2) is a two-weight $[\frac{N_1}{N}, m]$ linear code provided that $p^{\frac{m}{2}} + (-1)^t(N_2 - 1) > 0$, with two nonzero weights are given in Table V.

Table V. Weight distribution of C_D

Weight	Frequency
0	1
$\frac{p^m + (-1)^t(N_2 - 1)p^{\frac{m}{2}}}{pN_2}$	$\frac{p^m - 1}{N_2}$
$\frac{p^m - (-1)^t p^{\frac{m}{2}}}{pN_2}$	$\frac{(N_2 - 1)(p^m - 1)}{N_2}$

Theorem 1.2 is a generalization of Corollary 3.6. Now, we turn to the proof of Theorem 1.2.

Proof of Theorem 1.2 Let $x = x_0 + ux_1 + vx_2 + uvx_3$, where $x_0 \in D, x_1, x_2, x_3 \in \mathbb{F}_{p^m}$.

If $r = \beta uv \in M \setminus \{0\}$, where $\beta \in \mathbb{F}_{p^m}^*$, for a nonzero codeword $Ev(r) \in C(m, p)$, we have $\Phi(Ev(r)) = (tr(x_0\beta), tr(x_0\beta), tr(x_0\beta), tr(x_0\beta))_{x_0, x_1, x_2, x_3}$ and $w_L(Ev(r)) = w_H(\Phi(Ev'(r))) = 4p^{3m}(n - N(\beta))$, where $N(\beta) = |\{1 \leq j \leq n : tr(d_j\beta) = 0\}|$. Applying Formula (3), we know

$$\begin{aligned}
 n - N(\beta) &= n - \frac{n}{p} - \frac{\sum_{j=0}^{N_2-1} G(\bar{\varphi}^j, \chi) \varphi^j(b)}{pN_2} \\
 &= \frac{n(p-1)}{p} - \frac{-1 + \sum_{j=1}^{N_2-1} G(\bar{\varphi}^j, \chi) \varphi^j(b)}{pN_2} \\
 &= \frac{p^m}{pN_2} - \frac{\sum_{j=1}^{N_2-1} G(\bar{\varphi}^j, \chi) \varphi^j(b)}{pN_2}.
 \end{aligned}$$

Since

$$\left| \sum_{j=1}^{N_2-1} G(\bar{\varphi}^j, \chi) \varphi^j(b) \right| \leq (N_2 - 1)p^{\frac{m}{2}},$$

and $N_2 < p^{\frac{m}{2}} + 1$. So

$$4p^{3m-1} \frac{p^m - (N_2 - 1)p^{\frac{m}{2}}}{N_2} \leq w_L(Ev(r)) \leq 4p^{3m-1} \frac{p^m + (N_2 - 1)p^{\frac{m}{2}}}{N_2}.$$

Note that $n - N(\beta)$ is exactly the Hamming weight of the codeword of the cyclic code C_D . However, C_D has at most N_2 nonzero weights.

Hence, if r take over all the elements in $M \setminus \{0\}$, the codewords of $C(m, p)$ have at most N_2 different Lee weights.

If $r \in \mathcal{R}^*$. Let $r = r_0 + r_1u + r_2v + r_3uv$. The proof of this case is similar to that of Theorem 1.1. Hence, we can get $w_L(Ev(r)) = \frac{(p-1)s}{p} = 4p^{3m-1} \frac{p^m - 1}{N_2}$. Due to $4p^{3m-1} \frac{p^m - 1}{N_2} < 4p^{3m-1} \frac{p^m + (N_2 - 1)p^{\frac{m}{2}}}{N_2}$. Therefore, we have

$$\frac{4p^{3m-1} [p^m - (N_2 - 1)p^{\frac{m}{2}}]}{N_2} \leq d_L(C(m, p)) \leq \frac{4p^{3m-1} (p^m - 1)}{N_2}.$$

This completes the proof of Theorem 1.2. \square

Now we continue to give the proof of Theorem 1.3.

Proof of Theorem 1.3 Similar to the method of Theorem 1.1 and using the correlation content of Corollary 3.6, we can obtain Theorem 1.3. \square

4 The minimum distance of the dual code

A **linear code** C over R of length n is an R -submodule of R^n . For $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in R^n$, their standard inner product is defined by $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$, where the operation is performed in R . Let C be a linear code over R . The **dual code** C^\perp of C consists of all vectors of R^n which are orthogonal to every codeword in C , that is, $C^\perp = \{y \in R^n \mid \langle x, y \rangle = 0, \forall x \in C\}$.

We now describe the dual distance of the code $C(m, p)$ (resp. $C'(m, p)$) in the case we discussed in Theorem 1.1. To this end, we need the following lemma, its proof is similar to [22], we omit it here.

Lemma 4.1 If for all $r \in \mathcal{R}$, we have $Tr(rx) = 0$, then $x = 0$.

Next, we give the dual Lee distance of the two-Lee-weight codes $C(m, p)$.

Theorem 4.2 Let $C(m, p)^\perp$ (resp. $C'(m, p)^\perp$) be the dual of the code $C(m, p)$ (resp. $C'(m, p)$). If $N_2 = 1$, m is even or m is odd and $p \equiv 3 \pmod{4}$, for all $m \geq 1$, the Lee distance d^\perp (resp. d'^\perp) of $C(m, p)^\perp$ (resp. $C'(m, p)^\perp$) is 2.

Proof. First, we check that $d^\perp \geq 2$. This proof is similar to Theorem 6.2 in [21].

Next, we prove that $d^\perp < 3$. If not, applying the sphere-packing bound to $\Phi(C(m, p)^\perp)$, we can obtain $p^{4m} \geq 1 + s(p-1) = 1 + \frac{4p^{4m} - 4p^{3m}}{p-1}(p-1) = 1 + 4p^{4m} - 4p^{3m} > 4p^{4m} - 4p^{3m}$, then $4 > 3p^m$, a contradiction with the values of m and p , which implies $d^\perp < 3$. Hence, $d^\perp = 2$. Similarly, we can prove the Lee distance d'^\perp of $C'(m, p)^\perp$ is 2. \square

5 Optimality and Cryptography

5.1 Optimality of the p -ary image

Next, we study the optimality of image codes. Firstly, we recall the p -ary version of the Griesmer bound.

Lemma 5.1 [13] If $[\mathcal{N}, \mathcal{K}, \mathcal{D}]$ are the parameters of a linear p -ary code, then

$$\sum_{j=0}^{\mathcal{K}-1} \left\lceil \frac{\mathcal{D}}{p^j} \right\rceil \leq \mathcal{N}.$$

An $[\mathcal{N}, \mathcal{K}, \mathcal{D}]$ linear code C over \mathbb{F}_p is an \mathcal{K} -dimensional subspace of $\mathbb{F}_p^{\mathcal{N}}$ with minimum Hamming distance \mathcal{D} . An $[\mathcal{N}, \mathcal{K}, \mathcal{D}]$ linear code is called optimal if no $[\mathcal{N}, \mathcal{K}, \mathcal{D} + 1]$ code exists.

Theorem 5.2 Let m be positive integer and p be a odd prime. We have

- (a) if m is even or m is odd and $p \equiv 3 \pmod{4}$, then the codes $\Phi(C(m, p))$ are optimal with $N_2 = 1$;
- (b) if $m > 1$, the codes $\Phi(C'(m, p))$ are optimal.

Proof. (a) In our situation $\mathcal{N} = s = \frac{4p^{4m} - 4p^{3m}}{p-1}$, $\mathcal{K} = k = 4m$ and $\mathcal{D} = d = 4p^{4m-1} - 4p^{3m-1}$. when $p = 3$, by a simple calculation, we can obtain the codes $\Phi(C(m, p))$ are optimal. when $p > 3$, the ceiling function takes two values depending on the position of j .

- $0 \leq j \leq 3m - 1 \Rightarrow \lceil \frac{d}{p^j} \rceil = 4p^{3m-1-j}(p^m - 1)$,
- $3m \leq j \leq 4m - 1 \Rightarrow \lceil \frac{d}{p^j} \rceil = 4p^{4m-j-1}$.

Thus,

$$\begin{aligned}
 \sum_{j=0}^{k-1} \left\lceil \frac{d}{p^j} \right\rceil &= \sum_{j=0}^{3m-1} \left\lceil \frac{d}{p^j} \right\rceil + \sum_{j=3m}^{4m-1} \left\lceil \frac{d}{p^j} \right\rceil \\
 &= \sum_{j=0}^{3m-1} (4p^{3m-1-j}(p^m - 1)) + \sum_{j=3m}^{4m-1} (4p^{4m-j-1}) \\
 &= \frac{4p^{4m} - 4p^{3m}}{p-1} = s.
 \end{aligned}$$

(b) In our situation $\mathcal{N} = s' = 4(p^m - 1)p^{3m}$, $\mathcal{K} = k' = 4m$ and $\mathcal{D} = d' = 4(p-1)(p^{4m-1} - p^{3m-1})$.

when $p = 3$, by a simple calculation, we can get the codes $\Phi(C'(m, p))$ are optimal.

when $p > 3$, the ceiling function takes three values depending on the position of j .

- $0 \leq j \leq 3m - 1 \Rightarrow \lceil \frac{d+1}{p^j} \rceil = 4(p^{4m-j} - p^{3m-j} - p^{4m-j-1} + p^{3m-j-1}) + 1$,
- $j = 3m \Rightarrow \lceil \frac{d+1}{p^j} \rceil = 4(p^m - p^{m-1} - 1) + 1$,
- $3m + 1 \leq j \leq 4m - 1 \Rightarrow \lceil \frac{d+1}{p^j} \rceil = 4(p^{4m-j} - p^{4m-j-1})$.

Thus

$$\begin{aligned}
\sum_{j=0}^{k'-1} \left\lceil \frac{d'+1}{p^j} \right\rceil &= \sum_{j=0}^{3m-1} \left\lceil \frac{d'+1}{p^j} \right\rceil + \sum_{j=3m+1}^{4m-1} \left\lceil \frac{d+1}{p^j} \right\rceil + \left\lceil \frac{d+1}{p^{3m}} \right\rceil \\
&= \sum_{j=0}^{3m-1} (4(p^{4m-j} - p^{3m-j} - p^{4m-j-1} + p^{3m-j-1})) + 3m + \\
&\quad \sum_{j=3m+1}^{4m-1} (4(p^{4m-j} - p^{4m-j-1})) + 4(p^m - p^{m-1} - 1) + 1 \\
&= 4(p^{4m} - p^{3m}) + 3m - 3.
\end{aligned}$$

Note that $\sum_{j=0}^{k'-1} \left\lceil \frac{d'+1}{p^j} \right\rceil - s' = 4(p^{4m} - p^{3m}) + 3m - 3 - 4(p^m - 1)p^{3m} = 3m - 3 > 0$ with $m > 1$. The proof is completed. \square

Remark 2 The codes mentioned in Examples 3.4, 3.5 and 3.6 meet the conditions of the Theorem 5.2. Note that these codes are optimal ternary codes.

5.2 Application to secret sharing schemes

Secret sharing is an important topic in cryptography. It has been studied for over thirty years. In this section, we will study the secret sharing schemes based on the linear codes introduced in this paper.

• The access structure of the secret sharing schemes

A group of participants is referred to as a minimal access set if they can recover the secret by combining their shares, but none of its proper subgroups can. Thus, we are only interested in the set of all minimal access sets. A *minimal codeword* of a linear code C is a nonzero codeword that does not cover any other nonzero codeword. The support $s(x)$ of a vector x in \mathbb{F}_q^n is defined as the set of indices where it is nonzero. We say that a vector x covers a vector y if $s(x)$ contains $s(y)$. In fact, determining the minimal codewords of a given linear code is a difficult task. Here, we will present the Ashikhmin-Barg lemma [1], which is very useful in determining the minimal codewords, as follows.

Lemma 5.3 (Ashikhmin-Barg) Let w_{\min} and w_{\max} be the minimum and maximum nonzero weights of a q -ary code, respectively. If

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q},$$

then every nonzero codeword of C is minimal.

We can infer from there the support structure for the codes of this paper. Next, we obtain the result as follows.

Theorem 5.4 Let $m > 1$ and p be an odd prime. We have

- (a) if m is even or m is odd and $p \equiv 3 \pmod{4}$, then all the nonzero codewords of $\Phi(C(m, p))$ are minimal with $N_2 = 1$.
- (b) all the nonzero codewords of $\Phi(C'(m, p))$ are minimal.

Proof. (a) Applying Lemma 5.3, we know that $w_{\min} = \omega_1 = 4p^{4m-1} - 4p^{3m-1}$, and $w_{\max} = \omega_2 = 4p^{4m-1}$ in Table III. Then substituting these values into the inequality of Lemma 5.3 as $p\omega_1 > (p-1)\omega_2$, we can obtain

$$\begin{aligned} p\omega_1 - (p-1)\omega_2 &= p(4p^{4m-1} - 4p^{3m-1}) - 4(p-1)p^{4m-1} \\ &= 4p^{4m-1} - 4p^{3m} > 0, \end{aligned}$$

which is true for $m > 1$.

(b) Applying Lemma 5.3, we know that $w_{\min} = \omega'_1 = 4(p-1)(p^{4m-1} - p^{3m-1})$, and $w_{\max} = \omega'_2 = 4(p-1)p^{4m-1}$ in Table III'. Similar to the proof of the case (a), the conclusion is true for $m > 1$. \square

Theorem 5.5 Let m be even, and $2 < N_2 = \gcd(N, \frac{p^m-1}{p-1}) < p^{\frac{m}{2}-1}$, where $N|(p^m-1)$. Assume there exists a positive integer l , such that $p^l \equiv -1 \pmod{N_2}$. In addition, suppose that p , $\frac{m}{2l}$, and $\frac{p^l+1}{N_2}$ are all odd. Then all the nonzero codewords of $\Phi(C(m, p))$, for N_2 is even, are minimal.

Proof. By using Lemma 5.3, we know $w_{\min} = \frac{4p^{3m-1}[p^m - (N_2-1)p^{\frac{m}{2}}]}{N_2}$ and $w_{\max} = \frac{4p^{3m-1}[p^m + p^{\frac{m}{2}}]}{N_2}$ in Table II. Rewriting the inequality of Lemma 5.3 as $p w_{\min} > (p-1)w_{\max}$, and dividing both sides by $\frac{4p^{3m-1}}{N_2}$, we obtain

$$p(p^m - (N_2-1)p^{\frac{m}{2}}) > (p-1)(p^m + p^{\frac{m}{2}}),$$

or $N_2 p < p^{\frac{m}{2}} + 1$, which is true for $N_2 < p^{\frac{m}{2}-1}$. Hence, the theorem is proved. \square

• Massey's scheme

At the end of 1970s of the twentieth century, secret sharing schemes (SSS) were introduced by Shamir and Blakley. Later on, the constructions of linear codes with few weights have been studied. In fact, Massey's scheme [17] is a construction of such a scheme based on a code C of length s over \mathbb{F}_p and it is one of the famous SSS. In [17], Massey introduced the relationship between the access structure and the minimal codewords of the dual codes. In the favourable case that all nonzero codewords are minimal, it was shown in [8] that we have the following choice:

- (1) If $d^\perp \geq 3$, then the SSS is “*democratic*”: every user belongs to the same number of coalitions
- (2) If $d^\perp = 2$, then the SSS is “*dictators*”: users belong to every coalition.

By Theorems 4.2, 5.4 and 5.5, we see that for some values of the parameters, SSS built on $\Phi(C(m, p))$ (resp. $\Phi(C'(m, p))$) is dictatorial.

6 Conclusion

In the present paper, by the exploration and research of two different defining sets, we have obtained two classes of two-weight and three-weight linear codes from the trace codes over the ring $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. Furthermore, by employing the Griesmer bound, two families two-weight codes are shown to be optimal under some conditions on the parameters m and N_2 . Therefore, the selection of the defining sets decides the parameters of the codes. In addition, the dual Lee distance of the trace codes is also considered, and linear codes with few weights we construct have applications in SSS.

Compared with the codes we constructed by similar techniques in [4, 7, 9, 11], the p -ary linear codes we obtained from the trace codes over the ring in this paper are new. It is worth further investigating the weight distribution of the dual codes, their optimality, and their application to secret sharing schemes.

References

- [1] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Transactions on Information Theory, 1998, **44(5)**: 2010–2017.
- [2] E. Byrne, M. Greferath, T. Honold, Ring geometries, two-weight codes, and strongly regular graphs, Designs Codes and Cryptography, 2008, **48(1)**: 1–16.
- [3] A.R. Calderbank, J.M. Goethals, Three-weight codes and association schemes, Philips Journal of Research, 1984, **39(4)**: 143–152.
- [4] A.R. Calderbank, W.M. Kantor, The geometry of two-weight codes, Bulletin of the London Mathematical Society, 1986, **18(2)**: 97–122.
- [5] B. Courteau, J. Wolfmann, On triple sum sets and three-weight codes, Discrete Mathematics, 1984, **50(2-3)**: 179–191.

- [6] K. Ding, and C.S. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Transactions on Information Theory*, 2015, **61(11)**: 5835–5842.
- [7] C.S. Ding, C.L. Li, N. Li, Z.C. Zhou, Three-weight cyclic codes and their weight distributions, *Discrete Mathematics*, 2016, **339(2)**: 415–427.
- [8] C.S. Ding, J. Yuan, Covering and secret sharing with linear codes, *Lecture Notes in Computer Science*, 2003, **2731**: 11–25.
- [9] C.S. Ding, J. Yang, Hamming weights in irreducible cyclic codes, *Discrete Mathematics*, 2011, **313(4)**: 434–446.
- [10] T. Honold, I.N. Landjev, Linear codes over finite chain rings, *Electronic Journal of Combinatorics*, 2010, **7(1)**: 116–126.
- [11] Z.L. Heng, Q. Yue, A class of binary linear codes with at most three weights, *IEEE Communications Letters*, 2015, **19(9)**: 1488–1491.
- [12] Z.L. Heng, Q. Yue, A class of q -ary linear codes derived from irreducible cyclic codes, *arXiv:1511.09174v1*.
- [13] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, U.K., Cambridge University Press, 2003.
- [14] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge: Cambridge University Press, 1984.
- [15] J.E. MacDonald, Design methods for maximum minimum distance error-correcting codes, *Ibm Journal of Research & Development*, 1960, **4(1)**: 43–57.
- [16] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.
- [17] J.L. Massy, Minimal codewords and secret sharing. *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, Mölle, Sweden, 1993, pp. 276–279.
- [18] M.J. Shi, Y. Liu, P. Solé, Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Communications Letters*, 2016, **20(12)**: 2346–2349.
- [19] M.J. Shi, Y. Liu, P. Solé, Optimal two weight codes from trace codes over a non-chain ring, *Discrete Applied Mathematics*, doi.org/10.1016/j.dam.2016.09.050.
- [20] M.J. Shi, Y. Liu, P. Solé, Trace codes with few weights over $\mathbb{F}_p + u\mathbb{F}_p$, *arXiv:1612.00128v1 [cs.IT]*, Dec. 2016.

- [21] M.J. Shi, Y. Liu, P. Solé, Two-weight and three-weight codes from trace codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, arXiv:1612.00118v1 [cs.IT], Dec. 2016.
- [22] M.J. Shi, R.S. Wu, Y. Liu, P. Solé, Two and three-weight codes over $\mathbb{F}_p + u\mathbb{F}_p$, submitted to Cryptography and Communications-Discrete Structures, Boolean Functions and Sequences, doi:10.1007/s12095-016-0206-5, Sep. 2016.